UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/002,697	10/31/2001	Richard Paul Tarquini	10002019-1	4671

7590 04/06/2006

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
SON, LINH L D	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 04/06/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/002,697	TARQUINI, RICHARD PAUL	
	Examiner	Art Unit	
	Linh LD Son	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 January 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is responding to the Amendment received on 01/07/06.

2. Claims 1-20 are pending. Claims 1, 7 and 17 are amended.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-6, and 17-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Shanklin et al, US Patent No. 6487666, hereinafter "Shanklin".

5. As per claims 1 and 17:

Shanklin teaches "A method of identifying data in a network exploit, comprising: receiving a packet by an intrusion prevention system maintained by a node of a network (Col 2 lines 30-40), the intrusion prevention system bound to a media access control

driver and a protocol driver (Col 2 line 64 to Col 3 line 45); invoking a signature analysis algorithm by the intrusion prevention system (Col 3 lines 53-63, and Col 5 lines 18-40); utilizing parametric information to select a first rule set from a plurality of rules sets, the first rule set parametrically related to the packet (Col 3 lines 48-53, Col 4 lines 30-33, Col 5 lines 12-18, Col 5 lines 35-48, and Col 4 lines 30-33); and comparing the packet by the intrusion prevention system with the first rule set comprising a rule logically defining a packet signature (Col 5 lines 12-50).

6. As per claim 2:

Shanklin teaches "The method according to claim 1, wherein receiving a packet by an intrusion prevention system further comprises receiving a packet originating from the node" in (Col 5 lines 55-67).

7. As per claim 3:

Shanklin teaches "The method according to claim 1, wherein receiving a packet by an intrusion prevention system further comprises receiving a packet originating from a source external to the node, the packet addressed to the node" in (Col 5 lines 55-67).

8. As per claim 4:

Shanklin teaches "The method according to claim 1, further comprising discarding the packet upon determination that a signature of the packet corresponds to the rule" in (Col

4 lines 8-15).

9. As per claim 5:

Shanklin teaches "The method according to claim 1, wherein comparing the packet by an intrusion prevention system with a first rule set further comprises comparing the packet by the intrusion prevention system with a second rule set upon determination that a signature of the packet does not correspond to a rule of the first rule set" in (Col 5 lines 30-55).

10. As per claim 6:

Shanklin teaches "The method according to claim 1, wherein comparing the packet by the intrusion prevention system with a first rule set further comprises comparing the packet by the intrusion prevention system with a rule set comprising a plurality of rules each respectively comprising machine-readable code logically defining a packet signature" in (Col 5 lines 12-55).

11. As per claim 18:

Shanklin teaches "The computer readable medium according to claim 17, further comprising a set of instructions that, when executed by the processor, cause the processor to perform the computer method of determining whether a correspondence between a signature of the data packet and the at least one signature files exists" in

(Col 6 lines 44-55).

12. As per claim 19:

Shanklin teaches "The computer readable medium according to claim 17, further comprising a set of instructions that, when executed by the processor, cause the processor to perform the computer method of comparing the data packet with each signature file of the selected set of the plurality of signature files" in (Col 6 lines 44-55).

13. As per claim 20:

The computer readable medium according to claim 19, further comprising a set of instructions that, when executed by the processor, cause the processor to perform the computer method of: upon determining that no correspondence exists between the signature of the data packet and the signature files of the selected set of the plurality of signature files, selecting a second set of signature files from the plurality of sets of signature files; and comparing the signature of the data packet to at least one signature file of the second set of signature files" in (Col 6 lines 44-55).

Claim Rejections - 35 USC § 103

14. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

15. Claims 7-14, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shanklin.

16. As per claim 7:

Shanklin teaches "A node of a network maintaining an instance of an intrusion prevention system for identifying data in a network exploit, the node comprising: a central processing unit (Fig 1 #11, and Col 3 line 20-35); a memory module for storing data in machine-readable format for retrieval and execution by the central processing unit; and an operating system comprising a network stack comprising a protocol driver (Col 6 lines 20-28, Col 3 lines 25-34, Col 4 lines 50-55), a media access control driver and an instance of the intrusion prevention system bound to the protocol driver and the media access control driver (Col 3 lines 20-33, and lines 48-53), the intrusion prevention system comprising an associative process engine (Sensor Engine) and an input/output control layer (Ethernet Interface), the input/output control layer operable to receive a signature file generated from a network exploit rule (Col 3 lines 20-33, Col 6 lines 48-50)

comprising an operand (Col 5 line 19, and line 29), an operator (Col 4 lines 44-48, and Col 5 lines 43-50) and a mask (Col 3 lines 55-60), the input/output control layer operable to pass the signature file to the associative process engine (Col 6 lines 48-58), the associative process engine operable to utilize parametric information to select the signature file from a plurality of signature files, the signature file parametrically related to a data packet (Col 5 lines 12-18, Col 5 lines 35-48, and Col 4 lines 30-33), the associative process engine operable to analyze a data packet with the signature file and assign a logical value to the signature file dependent upon a result from the analysis (Col 5 lines 13-18, Col 6 lines 25-43).

However, Shanklin does not specifically disclose a memory module for storing data. Nevertheless, Shanklin does disclose the step of "matching stored signatures to received signatures" in (Col 6 lines 48-50). Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art at the time of the invention was made to realize that the memory module is explicitly disclosed in order to store the signature.

17. As per claim 8:

Shanklin teaches "The node according to claim 7, wherein the exploit rule further comprises a composite of a plurality of rules, each rule comprising an operand (Col 5 line 19, and line 29), an operator (Col 4 lines 44-48, and Col 5 lines 43-50) and a mask and having a logical value (Col 3 lines 55-60), each of the plurality of rules being logically connected with at least one of the other plurality of rules by a non-bitwise

boolean operator (Col 3 lines 20-33, and Col 6 lines 48-50), the logical value of the signature file dependent on the logical value of each of the plurality of rules" in (Col 5 lines 13-18, Col 6 lines 25-43).

18. As per claim 9:

Shanklin teaches "The node according to claim 7, wherein the operand comprises network frame data, the operator comprises a bitwise operation, and the mask comprises an operator mask" in (Col 9 lines 25-45).

19. As per claim 10:

Shanklin teaches "The node according to claim 7, wherein the network control layer is operable to receive a plurality of signature files each respectively generated from a network exploit rule" in (Col 6 lines 1-10).

20. As per claim 11:

Shanklin teaches "The node according to claim 10, wherein a parametric association is assigned to a subset of the plurality of signature files, the associative process engine operable to determine a parametric value of the packet and to analyze the packet with the subset of the signature files when the parametric association (Checksum verification) of the signature files coincide with the parametric value of the packet" in

(Col 3 lines 54-60).

21. As per claim 12:

Shanklin teaches "The node according to claim 11, wherein the parametric value of the packet is obtained from link-layer header information of the packet" in (Col 4 lines 29-33, and Col 3 lines 54-60).

22. As per claim 13:

Shanklin teaches "The node according to claim 11, wherein a plurality of parametric associations are respectively assigned to a plurality of subsets of signature files" in (Col 4 lines 29-33, and Col 3 lines 54-60).

23. As per claim 14:

Shanklin teaches "The node according to claim 11, wherein the parametric association is one of a plurality of parametric associations, each of the plurality of parametric associations (checksum) comprising a common subset of signature files, each signature file of the common subset respectively analyzed by the associative process engine against the network packet prior to analyzation of any other signature files of any other subsets of signature files" in (Col 4 lines 29-33, and Col 3 lines 54-60).

24. As per claim 16:

Shanklin teaches "The node according to claim 7, wherein the intrusion prevention system further comprises an intrusion event manager, the associative process engine operable to communicate that the analysis of the packet indicates a correspondence with the signature file, the intrusion event manager operable to generate an alert that is transmitted from the node to at least one of a management node in a network and an event database maintained by the node" in (Col 4 lines 8-15).

25. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shanklin in view of Vaidya, US Patent No. 6279113 (Cited in 892 dated 03/25/05).

26. As per claim 15:

Shanklin teaches "The node according to claim 10". However, Shanklin does not teach "further comprising a table maintained in the memory module, the table comprising a plurality of indices each respectively indexing a subset of the plurality of subsets of signature files". Nevertheless, Vaidya does disclose a signature database in (Col 2 lines 30-45). Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to realize that the signature database does including table of plurality of indices of signature files and its association.

Response to Arguments

27. Applicant's arguments filed 01/17/06 have been fully considered but they are not persuasive.

28. In regarding to the amended limitation in claim 1, 7, and 17, Applicant argues that the amended limitation, "utilizing parametric information to select a first rule set from a plurality of rules sets, the first rule set parametrically related to the packet", is not disclosed in Shanklin's invention. Examiner traverses Applicant's argument. In Col 3 lines 48-53, Col 4 lines 30-33, Col 5 lines 12-18, Col 5 lines 35-48, and Col 4 lines 30-33, Shanklin clearly teaches a method of utilizing the packet header information to associate with a signature for detection. It is clearly that Shanklin discloses the claimed invention.

Conclusion

29. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

30. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Linh LD Son whose telephone number is 571-272-3856. The examiner can normally be reached on 9-6 (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Linh LD Son
Examiner
Art Unit 2135

HOSUK SONG
PRIMARY EXAMINER